ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering
Tome VI (Year 2013) – FASCICULE 3 [July–September]
ISSN 2067–3809

[1.] Gunjan CHUGH

IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW ARTICLE

[1.] BANASTHALI VIDYAPITH, RAJASTHAN, INDIA

ABSTRACT: In today's world, since the rise of internet most of the communication and information sharing is done over the web. With the increasing unauthorized access of confidential data, information security is of utmost importance. Thus, a big issue now a day is to reduce the chances of information detection during transmission. Cryptography deals with encryption of message but its presence arouse suspicion about the communication, on the other hand, Steganography hides the existence of message in such a way that no one can even guess about the communication going on between two parties. Due to rapid development in both computer technologies and Internet, the security of information is regarded as one of the most important factors of Information Technology and communication. A large variety of Steganographic techniques exists for hiding data in digital images. In this paper, an overview on Steganography is presented and it also covers different existing techniques on Image Steganography and their relative strong and weak points. Steganography benefits and applications are also discussed.
KEYWORDS: Cover Image, Stego Image, Cryptography, Steganography

INTRODUCTION

Most of the time, users on the internet have to send, share or receive confidential information [1].

Due to rapid development in both computer technologies and Internet, the security of information is regarded as one of the most important factors of Information Technology and communication. Attacks on confidential data, unauthorized access of data have crossed the limits. Accordingly, we need to take measures which protect the secret information [2,3]. Steganography has emerged as a powerful and efficient tool which provides high level for security particularly when it is combined with encryption [4]

The general idea of hiding some information in digital content has a wider class of applications that go beyond steganography. The techniques involved in such applications are collectively referred to as information hiding. Two special cases of information hiding include digital watermarking and Fingerprinting. Watermarking can be used to provide copyright protection by extending the cover source with some extra information which can later be extracted and can be used for variety of purposes like copyright protection and control.

Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content [5].

In Fingerprinting, different customers are given different and specific marks embedded in the copies of their work. It helps to identify those customers who violate the licensing agreement when they transmit property to other groups illegally [4].

Steganography vs Cryptography

It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice [6]. Cryptography deals with the encryption of text to form cipher (encrypted) text using a secret key. However, the transmission of cipher text may easily arouse attackers suspicion, and the cipher text may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, an important sub-discipline of information hiding i.e Steganography has been developed as a new covert communication means in recent years. It transfers message secretly by embedding it into a cover medium with the use of information hiding techniques [7].

Steganography, hides the existence of message such that intruder can't even guess that communication is going on and thus provides a higher level of security than cryptography. Both cryptographic and steganographic systems provide secret communications, but they are different in terms of system breaking. If the intruder can read the secret message, then a cryptographic system is broken. However, a steganographic system is considered broken if the intruder can detect the existence or read the contents of the hidden message.

If the intruder suspects a specific file or steganography method even without decoding the message, a steganographic system will be considered to have failed. Thus, steganographic systems are

more fragile than cryptography systems in terms of system failure. [8]

Steganography

The word Steganography comes from the Greek origin, means "concealed (covered) writing". The word 'steganos' means "covered or protected" and 'graphie' means "writing" [9]. Steganography is thus, not only the art of information hiding, but also the art and science of hiding the fact that communication is even taking place.[10]

Due to the prohibition and restriction imposed by the government on cryptographic systems, Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Thus, Steganographic research is thus, primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment.

Steganography hides secret data in another file in such a way that only the recipient knows that such a message even exists. Neither Cryptography nor Steganography are sufficient, but using both technologies together can add multiple layers of security and provides a very acceptable amount of privacy for anyone connecting to and communicating over these systems. [11]

The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. On other hand, steganalysis is a way of detecting possible secret communication using against steganography. That is, steganalysis attempts to defeat steganography techniques. It is based on the fact that hiding information in digital media alters the carriers and introduces unusual signatures or some form of degradation that is visible to the human eye. Thus, it is crucial that a steganography system to ascertain that the hidden messages are not detectable [7].

Reasons for rapid growth of interest in Steganography

1.) Restrictions imposed on the availability of encryption service by various governments have encouraged people to take a move towards the methods through which messages can be embedded in cover sources.

2.) Publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products

STEGANOGRAPHY HISTORY

Information hiding is a science which dates back to 1499, and it has long history. It has been used in various forms for 2500 years. It has found use in military, diplomatic, personal, spies, ruler, governments etc. Steganography has been widely used, including in recent historical times and the present day. Some known examples include:

□ ***Past***

Early steganography was messy. Before phones, before mail, before horses, messages were sent on foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger. While information hiding techniques have received a tremendous attention recently, its application goes back to Greek times.

- according to Greek historian Herodotus, the famous Greek tyrant Histiaeus, while in prison, used unusual method to send message to his son-in-law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in-law. Herodotus provides the first records of steganography in Greece [13].
- to communicate Greeks would etch the message they wished to send into the wax.
- coating of a wooden tablet. The tablet would then be transported to the recipient who would read the message, then re-melt the wax to etch their reply. In order to communicate in secret, the army would remove the wax completely, carve the secret message into the wood, and re-coat the tablet with wax [13].
- Messages were also written on envelopes in the area covered by postage stamps to avoid the possible detection of the message.

□ ***Present***

In today's generation, as most of the people often transmit images, audio over the internet, so most of the Steganographic system's uses multimedia objects like image, audio and video as cover sources to hide the confidential data [14]. So, on the basis of this, steganography is divided into four categories:

1. Text Steganography
2. Image Steganography
3. Audio/Video Steganography
4. Protocol Steganography

□ ***Future***

Steganalysis can be defined as process to crack the cover object in order to get the hidden data. In general terms, it is known as Hacking i.e. unauthorized access of data during transmission. Future perspective of steganography lies on combining steganography with cryptography to achieve a higher level of security such that even if intruder detects the hidden message, he/she will not be able to decode it [14] .

STEGANOGRAPHY CLASSIFICATION

When we talk of digital steganography, we mean to say that, digital media's like Image, Audio /Video, Protocol are used as innocent covers for hiding secret confidential messages.

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [16]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [6]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of file formats that can be used for steganography. [2]

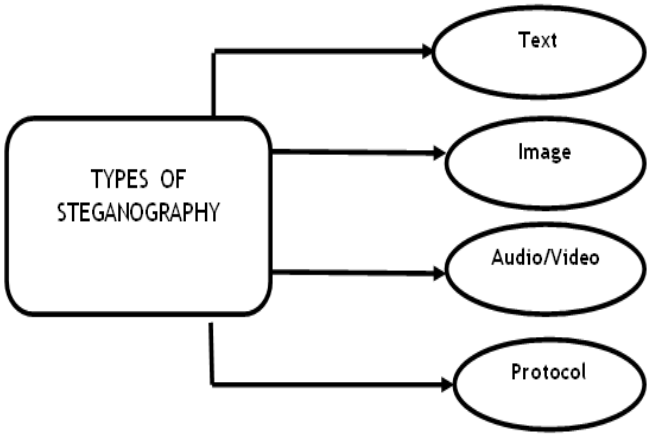

Figure 1: Classification of different types of Steganography

- ***Hiding information in text:***

Information can also be hidden in text files. The most popular method was to hide a secret message in every nth letter of every word of a text message [2]. A variety of different techniques exist of hiding data in text files. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

- ***Hiding information in images:***

Images are very popular cover source for digital steganography because of the large amount of redundant bits present in the digital representation of an image. This paper will focus on hiding information in images in the next sections.

- ***Hiding Information in Audio Files:***

Audio files can also be used for hiding secret data. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound [2].This property creates a channel in which to hide information.

The larger size of meaningful audio files makes them less popular to use than images [17].

- ***Hiding Information in Protocols:***

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [16]. In the layers of the OSI network model there exist covert channels where steganography can be used [19].

An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used. A paper by Ahsan and Kundur provides more information on this.[18, 2]

IMAGE STEGANOGRAPHY

The standard concept of "What You See Is What You Get (WYSIWYG)" which we encounter sometimes while printing images does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence, they can convey more than merely 1000 words [20].

The confidential data that is embedded should be of adequate quality in order to make it imperceptible and indecipherable.

In addition, the technique employed should facilitate the use of a high payload by the diligent embedding of more data in a given cover image [21].

BASIC CONCEPT

Steganography is a two-step process:

- *Step 1) Creating a stego image which is a combination of message and carrier*
- *Step 2) Extracting the message image from the stego image.*

Variations are in the techniques that are used to generate the stego image using the carrier and the message image. [21]

On the sender side, a Cover image is selected and then message is hidden using a secret key and message embedding algorithm. Secret key is basically used to find out the pseudorandom pixel locations where the data will be hidden. Secret key is to be shared between sender and receiver.

Thus, it works as password such that even if someone breaks the algorithm then also the message can't be extracted until he/she knows the secret key. Stego image is obtained as output (as shown in Figure 2).

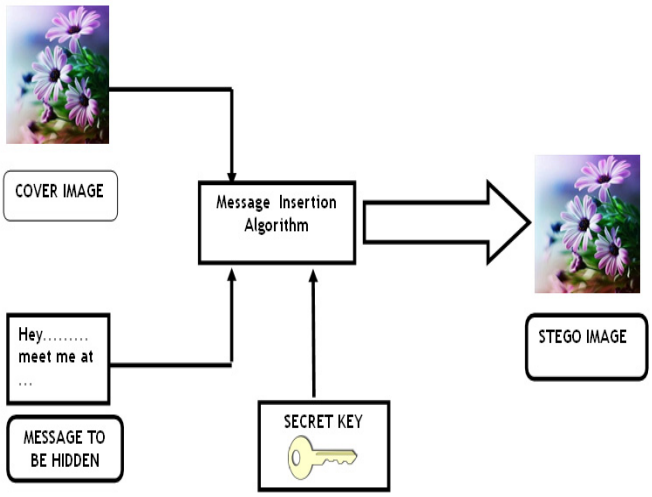

Figure 2: Image Steganography : Message Insertion

On the receiver side, Stego image is taken as input and by using the same secret key and message retrieval algorithm, message is extracted(as shown in Figure 3).

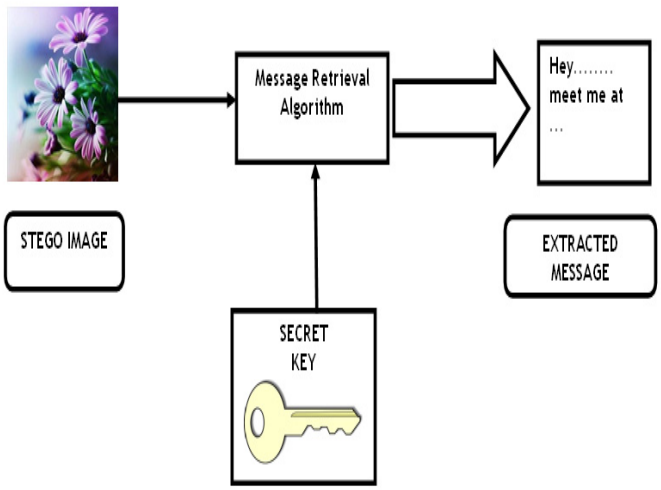

Figure 3: Image Steganography : Message Retrieval

FACTORS AFFECTING A STEGANOGRAPHIC SYSTEM

The effectiveness of any Steganographic method can be visualized by comparing Stego Image (Image after inserting message) with the Cover Image (Image before message insertion). Thus, some factors that determines how efficient and powerful a technique is are as follows:

1.) ***Robustness**: Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression [8].*

2.) ***Imperceptibility**: The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised[22]*

3.) ***Payload Capacity**: It refers to the amount of secret information that can be hidden in the cover source. Watermarking, needs to embed only a small amount of copyright information, on the other side, steganography aims at hidden communication and therefore requires sufficient embedding capacity [22].*

4.) ***PSNR (Peak Signal to Noise Ratio)**: It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [23, 24]. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed image.*

5.) ***MSE (Mean Square Error)**: Mean Squared Error is the average squared difference between a reference image and a distorted image. An Image steganography technique is efficient if it gives low MSE. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count [25].*

6.) ***SNR (Signal to Noise Ratio)**: It compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power [26].*

7.) ***NCC (Normalized Cross-Correlation)**: Normalized cross-correlation can be used to determine how to register or align the images by translating one of them. NCC is one of the methods used for template matching, a process used for finding incidences of a pattern or object within an image[27]*

8.) ***BER (Bit Error Rate)**: The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval [28].*

IMAGE STEGANOGRAPHY CLASSIFICATION

There are two popular schemes used for image steganography (shown in Figure 4): spatial domain embedding and transform domain embedding. Most of the steganographic techniques either use spatial domain or transform domain to embed the secret message [21].

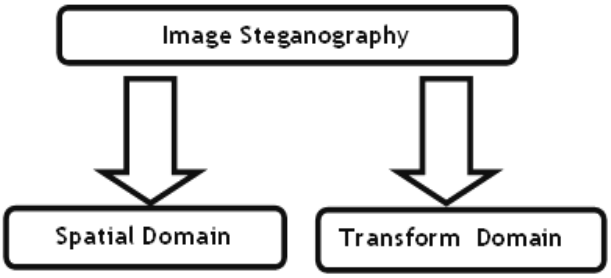

Figure 4: Image Steganography Classification

□ ***Spatial Domain***

In spatial domain scheme, the secret messages are embedded directly [10]. It embeds information in the intensity of the pixels [3]. We try to find out some areas or data that can be modified without having any significant effects on this cover file (Cole, 2003). Therefore, a secret message can be embedded by replacing the redundant or insignificant parts of a cover file with secret message bits, without adding any significant noise to this cover file (Kipper, 2004). [10]. The Least Significant Bit (LSB) substitution is the most commonly used spatial domain technique. In LSB substitution technique the least significant bit of each pixel of the cover is replaced by the secret message bits. Hiding images using LSB substitution techniques can be found in [21].

□ ***Transform Domain***

Transform Domain embeds information in frequency domain of previously transformed image [3]. Transform (frequency) domain techniques hide secret data in significant parts of the cover file. Therefore, frequency domain techniques are considered more robust to attacks than spatial domain techniques. Hence, most of robust steganographic systems known today rely on frequency domain techniques. There are many transforms used to map a signal into the frequency domain.

Discrete cosine transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT) are methods used as mediums to embed secret data in digital images. However, when we add a slight noise or secret data to some frequency domain components, it changes the whole image rather than changing only this part of the image. Thus, secret and embedded data will be spread across the entire image and will not be concentrated on one certain area or region [10].

DIFFERENT IMAGE STEGANOGRAPHY TECHNIQUES

□ ***LSB (Least Significant Bit) method** [8, 29, 30]*

It is one of the most common and easiest methods for message hiding. In this method, message is hidden in the least significant bits of image pixels .Changing the LSB of the pixels does not introduce much difference in the image and thus the stego image looks similar to the original image. In case of 24-bit images three bits of pixel can be used for LSB substitution as each pixel has separate components for red, green and blue.

Advantages:

1.) Simplest and easiest to implement.

2.) Chances of message insertion are 100%.

Drawbacks:

1.) *Not vulnerable to different attacks.*
2.) *Intruder can easily guess and change the LSB's of the image pixels, thus original message gets destroyed.*
3.) *Causes some distortion in the original image*
4.) *Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image will destroy the message*

□ ***Masking and Filtering*** *[8,29,30]*

Basically, this method is used for 24-bit and grey scale images. It is similar to placing watermarks on the image. Steganography only hides the information where as watermarks becomes part or attribute of the image. This method is more robust than LSB in terms of some image processing like - compression, cropping which makes it suitable in lossy JPEG images. Masking images involves changing the luminance of the masked area.

Advantages:

1.) Immune to image manipulation
2.) Robust technique

Drawbacks:

This method is mostly used for only 24 bit and grey scale images.

□ ***Parity Checker Method*** *[31]*

In this method, concept of even and odd parity is used. '0' is inserted at pixel value when it contains odd parity i.e. no. of 1's in the binary value of pixel must be odd Similarly, '1' is inserted at pixel value if it contains even parity i.e. no. of 1's in the binary value of the pixel must be even. If the corresponding parity does not exist at pixel location for 0 or 1 then it is made by adding or subtracting 1from the pixel value. For retrieval of message, if odd parity is present, then '0' is the message bit and if even parity is present, then '1' is the message bit.

Advantages:

1.) *Increases chances of message insertion.*
2.) *Steganalysis is difficult because whole pixel is used instead of particular bits as used by LSB method.*
3.) *Difference between cover image and stego image is difficult to be observed by naked eye.*

Drawbacks:

1.) *If intruder changes the LSB, then parity also changes and thus the method fails.*
2.) *In some situations when odd or even parity not present, then it can be made by both +1 or -1. So, it creates confusion, which one to choose.*

□ ***Gray Level Modification (GLM)*** *[15]*

In this technique, gray level values of the image pixels are modified. It provides one-to one mapping between the binary data and the selected pixels in an image. A set of pixels are selected from the image. First, all odd selected pixels are made even by changing gray level by one unit. Then, a comparison is made by selecting first bit from the message and first bit of the pixel.

If the first bit is even (0) then all pixels have even gray level and are not modified at all. But if the first bit is odd (1) then gray level of the pixel is decremented by one unit to make its value odd. Thus, Gray Level of all the pixels is modified accordingly.

Advantage:

Effective method as it can store as many bits as the size of the image

Drawback:

If LSB is damaged or changed by the intruder, then there is no concept of odd or even pixels and the method no longer works.

□ ***Pixel value Differencing (PVD) technique*** *[32]*

In this method, Wu & Tsai, selected two consecutive pixels for embedding the message. By checking the difference between two consecutive pixels ,payload of Wu and Tsai method is determined and it serves as basis to find out whether the two pixels belongs to an edge area or smooth area.

If the difference is large, it means pixels belong to an edge area and more secret data can be embedded at this location. On the other hand, if difference is small, it means pixels belong to smooth area and less secret data can be embedded at this place.

If the original difference value is unequal to the secret message, then the two consecutive pixels are directly adjusted so that the difference value can stand for the secret data [34].

Advantages:

1.) *Works better than LSB which directly embed secret data without considering the difference between the two pixels.*
2.) *Stego images produced are very much similar to the original image.*

Drawbacks:

1.) *Considerable stego image distortion can occur when the PVD method adjusts the two consecutive pixels in order to hide the secret data in the difference value.*
2.) *Falling off boundary problem may occur when the two consecutive pixels are located in extreme edge or smooth areas or when the values of two consecutive pixels form a contrast.*

□ ***Algorithms and Transformations***

This technique hides data in mathematical functions that are often used in compression algorithms. The idea of this method is to hide the secret message in the data bits in the least significant coefficients [33]. The advantage that JPEG images have over other formats is Compression. Using JPEG compression methods, high color quality images can be stored in relatively small files. JPEG images use the discrete cosine transform to achieve compression [29]. In addition to DCT, images can be processed with fast Fourier transformation and wavelet transformation. Other image properties such as luminance can also be manipulated.

Hidden information can be scattered through out the cover image using Patchwork and similar techniques such as spread spectrum methods. These approaches may help protect against image processing such as cropping and rotating, and they hide information more thoroughly than by simple masking.

By using redundant pattern encoding, a small message may be painted many times over an image so that if the stego image is cropped, there is a high probability that the watermark can still be read. A

large message may be embedded only once because it would occupy a much greater portion of the image area [29].

Advantages:

1.) Increases robustness, by using redundant pattern encoding i.e there is higher chance that message will be available after image manipulation.
2.) Message can easily be hidden in high colour quality JPEG images as they use DCT lossy compression transform.
3.) It also increases probability that only the intended receiver will be able to decode the message as message is encrypted and scattered through out the image.[3]

Drawbacks:

1.) This method uses frequency domain techniques such as cosine transform, wavelet transform and Fourier transform which are not so easy to implement.
2.) As using this technique, message is spread through out the image, so adding a slight noise may change the whole image rather than only the parts where data is hidden.

BENEFITS OF STEGANOGRAPHY [11]

1. Cryptography only encrypts the message and thus provides a clue to the intruder that communication is going on. Steganography on the other hand conceals the existence of message in some cover source, such that no one can guess that message is being hidden in some cover source.
2. Watermarking, another useful concept can also be implemented using Steganography. Watermarking can be used to provide copyright protection by extending the cover source with some extra information. Steganography can be used to maintain the confidentiality of valuable information to protect the data from possible sabotage, theft.
3. In today's world, all the transactions, shopping, banking, reservations are done over the web so it is very much essential to keep confidential information secret like credit card numbers, debit cards and personal bank accounts. All this can easily be done by hiding these confidential data in a cover source using digital Steganography.

DRAWBACKS OF STEGANOGRAPHY [17]

1. Steganography hides a message, but if someone knows the message is there, the message can be read. To avoid this, cryptography combined with steganography is used. For example, the message could be encrypted before it is hidden. Therefore, even if the message is found, it cannot be read.
2. If someone suspects that Steganography is being used, hidden message can be destroyed. For example, if data is hidden within an image, the message is usually inserted into the least significant bits. Therefore, if the bit composition changes even slightly, the message is destroyed.
3. Another limitation is due to the size of the medium being used to hide the data. Message should be hidden in such a way that it requires minimum changes in cover source in which it is embedded.

APPLICATIONS [8]

□ ***Secret Communication***

Using Steganography, two parties can communicate secretly without anyone knowing about the communication. Cryptography, only encode the message but its presence is not hidden and thus draws unwanted attention, Steganography, thus, on the other hand, hides the existence of message in some cover media. Steganography provides us with [35]:

1. Potential capability to hide the existence of confidential data
2. Hardness of detecting the hidden (i.e., embedded) data
3. Strengthening of the secrecy of encrypted data

□ ***Copyright Protection***

This is basically related to watermarking i.e a secret message is embedded in the image which serves as the watermark and thus identify it as an intellectual property which belongs to a particular owner.

□ ***Feature Tagging***

Features such as captions, annotations, name of the individuals in a photo or location in a map can be embedded inside an image. Copying the stego image also copies all of the embedded features and only parties who possess the decoding stego key will be able to extract and view the features [9].

□ ***Digital Watermarking***

This is one of the most important applications of Steganography. It basically embeds a digital watermark inside an image. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication [35]

□ ***Use by terrorists***

Steganography at a large scale can also be used by terrorists, who hide their secret messages in innocent, cover sources to spread terrorism across the country. Rumours were spread about terrorists using steganography when the two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption" were published in newspaper. Other media worldwide cited these rumours many times, especially after the terrorist attack of 9/11, without ever showing proof.[36]

□ ***Other Applications***

Steganography is widely used in areas such as Military, Banking, Market Applications to provide secure communication between the parties. In Industries, Steganography is widely used as a mechanism to prevent piracy. It is also used in biometrics for providing secure and robust biometrics system

CONCLUSIONS

In this paper, an overview on Steganography is described. How Steganography differs from cryptography is also discussed. In the former, message is hidden in the cover source where as in the later message is only encrypted but it is visible during the transmission. Different techniques on image steganography with their relative pros and cons such as Least Significant Bit (LSB), Making and Filtering, Parity Checker Method, Gray Level

Modification (GLM) method are also discussed. The paper also covers steganography benefits, drawbacks and different applications such as secret communication, copyright protection, digital watermarking.

REFERENCES

[1.] *Arvind Kumar and Km. Pooja "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 - 8887) ,Volume 9- No.7, November 2010*

[2.] *T. Morkel , J.H.P. Eloff and M.S. Olivier "An Overview of Image Steganography"*

[3.] *Amanpreet Kaur, Renu Dhir, and Geeta Sikka "A New Image Steganography Based On First Component Alteration Technique" (IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 3, 2009*

[4.] *Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi "Image Steganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012*

[5.] *Mehdi Kharrazi, Husrev T. Sencar and Nasir Memon "Image Steganography : Concepts and Practices "Polytechnic University, Brooklyn, NY 11201, USA*

[6.] *Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "Information Hiding A Survey"Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.*

[7.] *Ankita Agarwal " Security Enhancement Scheme for Image Steganography using S-DES Technique" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 4, April 2012*

[8.] *Adel Almohammad "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility" A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing , Brunel University, August, 2010.*

[9.] *Rajkumar Yadav "Study of Information Hiding Techniques and their Counterattacks: A Review Article" , International Journal of Computer Science & Communication Networks, Vol 1(2), 142-164, Oct-Nov 2011*

[10.] *Angela D. Orebaugh " Steganalysis: A Steganography Intrusion Detection System" , George Mason University*

[11.] *Bret Dunbar, "A detailed look at Steganographic Techniques and their use in an Open- Systems Environment", SANS Institute InfoSec Reading Room, SANS Institute 2002*

[12.] *Jagvinder Kaur, Sanjeev Kumar "Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011*

[13.] *www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf "Image Steganography and Steganalysis*

[14.] *Samir K Bandyopadhyay, Debnath Bhattacharyya[1], Debashis Gangul[1], Swarnendu Mukherjee[1] and Poulami Das[1] "A Tutorial Review on Steganography" University of Calcutta, Senate House, 87 /1 College Street, Kolkata - 700073 , [1]Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata - 700107 , IC3-2008*

[15.] *Ahmad T. Al-Taani and Abdullah M. AL-Issa "A Novel Steganographic Method for Gray-Level Images" International Journal of Computer and Information Engineering 3:1 2009*

[16.] *W Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, Vol. 35, No. 3 and 4, pp. 313-336, 1996.*

[17.] *Eric Cole "Stego Marking Packets to Control Info. Leakage on TCP/IP Based Networks"*

[18.] *Rengarajan Amirtharajan, Aishwarya G, Madhumita Rameshbabu, John Bosco Balaguru Rayappan, "Optimum Pixel & Bit location for Colour Image Stego- A Distortion Resistant Approach", International Journal of Computer Applications (0975 - 8887),Volume 10- No.7, November 2010*

[19.] *Abbas Cheddad " Strengthening Steganography in Digital Images" ,School of Computing and Intelligent Systems, Faculty of Engineering, University of Ulster, Magee*

[20.] *Abbas Cheddad, JoanCondell, KevinCurran, PaulMcKevitt "Digital image steganography: Survey and analysis of current methods" Signal Processing 90 (2010) 727-752*

[21.] *Saurabh V. Joshi ,Ajinkya A. Bokil, Nikhil A. Jain, Deepali Koshti "Image Steganography Combination of Spatial and Frequency Domain" International Journal of Computer Applications (0975 - 8887) Volume 53- No.5, September 2012*

[22.] *T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier " An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group ,Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa*

[23.] *http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio "Peak Signal to Noise Ratio"*

[24.] *http://wiki.answers.com/Q/What_is_psnr_in_steganography "PSNR in Steganography"*

[25.] *http://tdistler.com/iqa/algorithms.html "Mean Square Error"*

[26.] *http://en.wikipedia.org/wiki/Signal-to-noise_ratio "Signal-to-Noise Ratio"*

[27.] *http://www.mathworks.in/help/images/examples/registering-an-image-using-normalized-cross-correlation.html "Normalized Cross Co-relation"*

[28.] *http://en.wikipedia.org/wiki/Bit_error_rate "Bit-Error Rate"*

[29.] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEE Computer, Feb 1998, pp 26-34.

[30.] Rajkumar Yadav "Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters" Int. J. Comp. Tech. Appl., Vol 2 (6),1867-1870, NOV-DEC 2011

[31.] Rajkumar , Rahul Rishi , Sudhir Batra " A New Steganography Method for Gray Level Images using Parity Checker" International Journal of Computer Applications (0975 – 8887) Volume 11– No.11, December 2010

[32.] Chung-Ming Wang , Nan-I Wu , Chwei-Shyong Tsai , Min-Shiang Hwang, "A high quality steganographic method with pixel-value differencing and modulus function" J. Syst. Software (2007), doi:10.1016/j.jss.2007.01.049

[33.] Khan, Mohammed Minhajuddin , "Steganography"

[34.] G.Rupesh Kumar "Steganography", Seminar Report, Balaji Institute of technology and Sciences, Deptt. of Computer Science and Engg. Narsampet, Warangal, March 2011

[35.] Applications of Steganography http://www.datahide.com/BPCSe/applications-e.html

[36.] http://en.wikipedia.org/wiki/Steganography

ISSN: 2067-3809 [CD-Rom, online]